MAANPUOLUSTUSKORKEAKOULU

VIRANOMAISVERKON TIETOTURVALLISUUS

Kandidaatintutkielma

Kadetti
Jani Fabian Linderoos

97. Kadettikurssi
Maavoimien johtamisjärjestelmälinja

maaliskuu 2013

MAANPUOLUSTUSKORKEAKOULU

Kurssi	Linja
97. Kadettikurssi	Maavoimien johtamisjärjestelmälinja
Tekijä Kadetti Jani Fabian Linderoos	
Tutkielman nimi **Viranomaisverkon tietoturvallisuus**	
Oppiaine, johon työ liittyy Sotatekniikka	Säilytyspaikka Kurssikirjasto (MPKK:n kirjasto)
Aika maaliskuu 2013	Tekstisivuja 26 Liitesivuja 1

TIIVISTELMÄ

Viranomaisverkko on TETRA-standardin mukaan rakennettu digitaalinen radioverkko. Sen vaatimuksia ovat nopeus, monikäyttöisyys ja turvallinen kommunikointi. Nopeaan tahtiin kehittyvä tietotekniikka ja jatkuvasti kehittyvä kryptoanalyysi aiheuttavat tietoturvaominaisuuksien nopeaa vanhenemista. Tämän takia tulee analysoida tietoturvallisuusominaisuuksia tasaisin väliajoin.

Tutkimuksen päätutkimuskysymyksenä on, miten on varmistettu, että viranomaisverkossa lähetetty tieto ei pääse sivullisten käytettäväksi. Tämän lisäksi tutkimuksessa vastataan alatutkimuskysymyksiin, riittääkö viranomaisverkon salaus muodostamaan murtamisesta taloudellisesti kannattamatonta ja riittääkö salaus myös lähitulevaisuudessa estämään salakuuntelun. Tutkimus on suoritettu pääasiassa kirjallisuusselvityksenä.

TETRA-standardissa tietoturva perustuu perustason ja ylemmän tason tietoturvaan. Perustaso käsittää molemminpuolisen tunnistamisen sekä radiopuhelimien salakuuntelun estävän ilmarajapinnan salauksen. Ylemmän tason salaus on tarkoitettu puheen ja datan päästä päähän -salamiseen. Salauksia tarkasteltaessa tulee muistaa, että täysin varmaa salausjärjestelmää ei ole olemassa, on vain kyse siitä, kuinka paljon aikaa ja rahaa ollaan valmiita kuluttamaan sen murtamiseen. Perustason turvallisuus on murrettavissa lähitulevaisuudessa brute forcen avulla, mutta ylemmän tason salauksen purkamiseen vaaditaan onnistunutta kryptoanalyysiä tai tulevaisuuden kvanttitietokoneiden laskentakapasiteettia. Tunnistusmekanismia vastaan voidaan hyökätä esimerkiksi kloonaamalla päätelaite.

AVAINSANAT
TETRA, Virve, tietoturvallisuus, päästä päähän -salaus, ilmarajapinta, IDEA, brute force, Molemminpuolinen tunnistusmekanismi

VIRANOMAISVERKON TIETOTURVALLISUUS

SISÄLLYS

LYHENTEET

AC	Authentication Code
AI	Air-Interface
BS	Base station
CCK	Common Cipher Key
DCK	Derived Cipher Key
DMO	Direct Mode Operation
EDA	European Defence Agency
ETSI	European Telecommunications Standards Institute
FLOPS	Floating point operations per second
GCK	Group Cipher Key
GW	Gateway Interface
IDEA	International Data Encryption Standard
ISI	Inter-System-Interface
ISSI	Individual Short Subscriber Identity
ITSI	Individual Tetra Subscriber Identities
LSI	Line Station Interface
MS	Mobile station
NMSI	Network Management System Interface
OTAR	Over The Air Re-Keying
PEI	Peripheral Equipment Interface
SCK	Static Cipher Key
TETRA	Terrestrial Trunked Radio
UAK	User Authentication Key

VIRANOMAISVERKON TIETOTURVALLISUUS

1 JOHDANTO

Viranomaisverkko VIRVE on TETRA-standardin (Terrestrial Trunked Radio) mukainen EDA:n (European Defence Agency) infrastruktuurilla toteutettu radioverkko eri viranomaisten ja julkishallinnon organisaatioiden käyttöön. Viranomaisverkon pääkäyttäjiä ovat Poliisi, Tulli, Rajavartiolaitos, Palo- ja pelastuslaitos, Tielaitos, sosiaali- ja terveyspalvelut, merenkulkulaitos, Ilmailulaitos sekä Puolustusvoimat. Verkon rakentaminen aloitettiin vuonna 1998, ja se on nykyään koko Suomen kattava verkko. Viranomaisverkolle asetettuja vaatimuksia ovat nopeus, monikäyttöisyys ja turvallinen kommunikointi. [20; 40; 41]

Viranomaisverkon tietoturvallisuus perustuu TETRA-standardiin, joka tukee kaksitasoista tietoturvaa. Tietoturva perustuu perustason ja ylemmän tason tietoturvaan. Perustaso käsittää molemminpuolisen tunnistamisen sekä radiopuhelimien salakuuntelun estävän ilmarajapinnan salauksen. Ylemmän tason salaus on tarkoitettu puheen ja datan päästä päähän -salamiseen, jonka avulla TETRA-verkkoa voidaan muun muassa välittää muissa verkoissa. [20; 22]

1.1 Tutkimuksen näkökulmat ja rajaukset

Pääasiallinen tavoite on tutkia VIRVE-verkon tietoturvallisuutta. Tutkimus on tehty teknisestä näkökulmasta ja siinä käsitellään viranomaisverkon tietoturvaratkaisuja. Tutkimuksessa esitellään TETRA-standardin ja VIRVE-verkon yleistä rakennetta niin paljon kuin se on tutkielman kokonaisuuden ymmärtämisen kannalta välttämätöntä. Tutkimuksen painopisteenä ovat salaukset ja niiden toteutukset. Salauksien kestävyyttä tarkastellaan purkamiseen kuluvan ajan, purkamistyöhön ja laitteistoon tarvittavien resurssien näkökulmasta.

Tutkimusongelmana on Viranomaisverkon salauksien riittävyys luottamuksellisen tiedon siirtämiseen nykyaikana ja lähitulevaisuudessa. Jatkuvasti kasvavan tietokoneiden laskentakapa-

siteetin ansiosta salausavaimien pituuden merkitys kasvaa. Lisäksi kokemuspohjaisesti voidaan sanoa, että algoritmit vanhenevat ajan myötä ja menettävät samalla tehonsa. Esimerkkinä salauksen tehon menettäneestä verkosta on GSM-verkko [42].

Tutkimusongelmasta muodostuu tutkielman pääkysymys ja siihen liittyvät seuraavat alakysymykset:
– Miten on varmistettu, että viranomaisverkossa lähetettävä tieto ei pääse sivullisen käytettäväksi?
– Riittääkö viranomaisverkon salaus muodostamaan sen murtamisesta taloudellisesti kannattamatonta?
– Riittääkö salaus myös lähitulevaisuudessa estämään salakuuntelun?

Päätutkimuskysymykseen vastataan toisessa kappaleessa, jossa käsitellään TETRA-standardin asettamat tietoturvaratkaisut viranomaisverkolle. Kolmannessa kappaleessa vastataan alatutkimuskysymyksiin. Tutkimuksessa keskitytään ainoastaan tiedon luottamuksellisuuteen.

Salauksen riittävyydellä tarkoitetaan, että sen murtaminen on taloudellisesti kannattamatonta. Kannattamattomuus luokitellaan tässä tutkimuksessa siten, että voidaan olettaa, että yksittäiset henkilöt tai pienten organisaatioiden varallisuudet eivät riitä tarvittavan laskentakapasiteetin tai ammattitaidon hankkimiseen. Tutkielmassa ei käsitellä tietoturvallisuuteen liittyvää häirintää, fyysistä tuhotyötä, käyttäjävirheitä, salauksen käytettävyyttä, eikä verkon dataliikenteen virheisiin liittyviä seikkoja, koska tutkielman tarkoituksena on tutkia viestien luottamuksellista lähettämistä todennuksen ja salauksen näkökulmasta. Lähitulevaisuudella tarkoitetaan tässä tutkimuksessa seuraavaa kymmentä vuotta, eli vuoteen 2023 saakka. Kolmannen luvun osio 3.1.2 ”*Algoritmien kestävyys ja luotettavuus*” käsitellään teoreettisella tasolla. Kandidaatintutkielman suppeuden ja algoritmien salaisuuden vuoksi luku käsitellee tunnettuja algoritmeja. Tässä tutkimuksessa oletetaan algoritmien vastaavan vahvuudeltaan viranomaisverkossa käytettäviä algoritmeja. Tutkimuksessa pyritään löytämään keinoja, joilla salaista algoritmia vastaan voidaan hyökätä, sekä analysoimaan algoritmin salassapitoon liittyviä etuja ja haittoja.

1.2 Tutkimusmenetelmät ja tarpeellisuus

Tutkimus perustuu ensisijaisesti kirjallisuusselvitykseen. Lähteinä on pääasiassa käytetty aiheesta julkaistuja tutkielmia, tietoturvallisuusalan kirjallisuutta ja ETSI-asiakirjoja (European Telecommunications Standards Institute). Muita lähteitä ovat internetlähteet sekä Puolustus-

voimien asiakirjat. Asiakirjat ja Maanpuolustuskorkeakoulun julkaisemat lähteet ovat hyvin luotettavia sisällöltään, koska ne ovat virallisia asiakirjoja. Ongelmana kirjallisuusselvityksessä on lähteiden ajankohtaisuus. Monet tässä työssä käytettävät lähteet on julkaistu edellisellä vuosikymmenellä ja ovat siten vanhoja, eikä aiheesta ole välttämättä sen jälkeen julkaistu luotettavia aineistoja. Tässä työssä lähdekritiikki nousee esiin nimenomaan ajankohtaisuutta tarkasteltaessa. Tulevaisuutta koskevissa osioissa on oltava kriittinen sen ennustamiseen perustuvan luonteen vuoksi.

Viranomaisverkon tietoturvallisuudesta ei ole tehty useita tutkimuksia. Ilkka Korkiamäen ”TETRA-järjestelmän sotilaalliset käyttömahdollisuudet” on näistä yksi laajimmista. Tämän tutkimuksen lähdemateriaalin pohjana on ETSI-asiakirjat, sillä viranomaisverkon salaukset perustuvat TETRA-standardin käyttämiin ETSI:n standardeihin. Standardien lisäksi käytetään Korkiamäen tutkimusta, josta löytyy ETSI:n asiakirjoista löytyvä tieto suomeksi ja tiivistetysti.

Tutkimus on tarpeellinen, koska viranomaisverkon tietoturvallisuutta tulee arvioida tietyin väliajoin. Tietokoneiden kapasiteettien kasvun myötä myös salauksien kestävyys tulee arvioida ajankohtaisesti. Tietokoneiden kapasiteetti ja vuokrattava laskentateho mahdollistaa muun muassa brute forcen käyttömahdollisuuden ja toimivuuden paranemisen. Tämän lisäksi on hyvä arvioida algoritmien kestävyyttä teoreettisella tasolla ja arvioida niiden luotettavuutta lähitulevaisuudessa jo murtuneiden algoritmien esimerkkien avulla.

1.3 Keskeiset käsitteet

Autentikointi: Autentikointi eli haastemenetelmä on todennuksen menetelmä, jossa kutsuttu palvelin tai viestin saaja pyrkii varmistumaan kutsujan tai lähettäjän aitoudesta ottamalla tähän uuden yhteyden tai esittämällä tälle kysymyksen, johon vain oikea taho voi vastata oikein. [38]

Brute force attack: Brute force attack on vapaasti suomennettuna “raa´an voiman hyökkäys”. Brute force -hyökkäystä käytetään salasanojen murtamiseen ja sen pohjalta on tehty useita eri ohjelmia. Sen toimintaperiaate on kaikkien mahdollisten avainten tai salasanojen systemaattinen kokeilu salakirjoituksen avaamiseksi tai salasanan löytämiseksi [38]. Menetelmä on työläs, mutta toimiva. Tietokoneiden kehityksen ja vuokrattavan laskentatehon myötä brute force on jatkuvasti tehostuva keino.

ETSI: European Telecommunications Standards Institute on voittoa tavoittelematon standardisoimisjärjestö, joka tuottaa maailmanlaajuisesti sovellettavia standardeja tieto- ja viestintätekniikoihin. ETSI on Euroopan unionin virallisesti hyväksymä standardointiorganisaatio. [12]

Iterointi: Tässä tutkimuksessa iteroinnilla tarkoitetaan menetelmää, jossa toistetaan laskutoimituksia. [36]

Luottamuksellinen: Luottamuksellisella tarkoitetaan tässä tutkimuksessa, että tiedot ovat vain haluttujen, rajoitettujen henkilöiden saatavissa eivätkä ne paljastu sivullisille.

Mooren laki: Mooren lailla tarkoitetaan tietokoneiden transistoreiden määrän kaksinkertaistumista noin 1,5 vuoden välein, mikä tarkoittaa käytännössä tietokoneen laskentatehon kaksinkertaistumista samassa ajassa. [16]

Salausalgoritmi: Tässä tutkimuksessa salausalgoritmilla tarkoitetaan matemaattista algoritmia, jonka avulla selväkielinen (plaintext) teksti muutetaan salattuun muotoon (ciphertext). [29]

Tetra: TETRA (Terrestial Trunked Radio) on ammattikäyttöön tarkoitettu digitaalinen matkapuhelinjärjestelmä, joka tukee puheensiirtoa ja tiedonsiirtoa sekä pakettikytkentäisenä että piirikytkentäisenä. VIRVE-verkko perustuu TETRA-standardiin. [20]

Tietoturvallisuus: Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien ja palvelujen suojaamista sekä normaali- että poikkeusoloissa hallinnollisten ja teknisten toimenpiteiden avulla. Tietoturvallisuus muodostuu tiedon kolmen ominaisuuden – luottamuksellisuuden, eheyden ja käytettävyyden – turvaamisesta. [15]

2 VIRANOMAISVERKKO

Tässä kappaleessa esitellään viranomaisverkon yleistä rakennetta, sen tarjoamia palveluita ja tietoturvaratkaisuja. Viranomaisverkko pohjautuu TETRA-standardiin, minkä vuoksi standardin esittely on välttämätöntä. Kappaleen sisältö perustuu pitkälti Ilkka Korkiamäen kirjaan ”TETRA-järjestelmän sotilaalliset käyttömahdollisuudet” ja ETSI:n standardeihin.

2.1 TETRA-standardi

TETRA (Terrestial Trunked Radio) on trunking-tekniikkaan perustuva ETSI:n (European Telecommunications Standatrds Institute) määrittelemä digitaalinen radioverkko [27]. TETRA-standardin valmistelu käynnistettiin 1980-luvun loppupuolella. Vuonna 1990 ETSI pyysi laitevalmistajia valmistelemaan omat ehdotuksensa TETRA-teknologiaksi. Ehdotuksiin vastasi yhteensä kuusi valmistajaa, muun muassa Nokia ja Motorola. Ehdotuksien pohjalta ETSI valitsi TETRA-teknologian vuonna 1991, minkä jälkeen alkoi standardointityö, joka valmistui vuonna 1995, kun ensimmäinen versio julkaistiin. [41]

TETRA-standardissa on kaksi verkkotyyppiä, jotka käyttävät samaa rajapintaa, mutta eivät kuitenkaan ole toistensa kanssa yhteensopivia fyysisellä kerroksella. Yhteensopivuus on määritelty verkkotyypeille verkkokerroksella. Verkkotyypit ovat: Voice + Data, joka tarjoaa yhdistetyt puhe- ja datasiirtopalvelut, ja TETRA Packet Data Optimized, joka tarjoaa ainoastaan pakettivälitteisen datasiirtopalvelun. Viranomaisverkko on toteutettu Voice + Data -standardin mukaisesti. [20]

2.1.1 Rajapinnat

TETRA-standardissa on määritelty verkon toiminnalliset rajapinnat, muu toteutus jää laitevalmistajalle. TETRA-standardin rajapinnat ovat

- AI (Air-Interface) eli ilmarajapinta, järjestelmän infrastruktuurin ja radioiden välillä.
- PEI (Peripheral Equipment Interface) eli oheislaiterajapinta datalaitteiden liittämiseksi radioihin.
- ISI (Inter-System-Interface) eli kahden eri TETRA-verkon välinen rajapinta.
- DMO (Direkt Mode Operation) eli suorakanavarajapinta, joka on ilman verkkoa tapahtuvaa kahden päätelaitteen välistä liikennöintiä varten

- NMSI (Network Management System Interface) eli verkon käytönohjaukseen ja hallintaan käytettävä verkonhallintarajapinta.
- LSI (Line Station Interface) eli lankaliittymän rajapinta.
- GW (Gateway Interface) eli yhdyskäytävärajapinta on TETRA-verkon liittämiseksi ulkoisiin verkkoihin. [20]

Tässä tutkimuksessa tärkein rajapinta on AI eli ilmarajapinta, koska ilmateitse kulkeva viesti on helpointa siepata.

Trunking-tekniikka mahdollistaa sitoutumattomuuden tiettyyn radiokanavaan, koska järjestelmä etsii ja antaa tiedonsiirrolle vapaan aikavälin ja tarvittavan tukiaseman kanavaryhmästä [20]. TETRA-standardi määrittelee seuraavat erilaiset trunking-menetelmät, joista laitevalmistajat voivat valita käyttöönotettavat:

- **Message trunking** -menetelmässä kanava on jatkuvasti varattu saman lähetyksen ajaksi. Yhteys katkaistaan vasta, kun puhelunomistaja selvästi lopettaa puhelun tai aktiivisuusajastin menee umpeen.
- **Transmission trunking** -menetelmässä kanava varataan ainoastaan jokaista lähetystä varten. Lähetyskanavan varaus lopetetaan välittömästi lähetyksen päätyttyä.
- **Quasi-transmission trunking** -menetelmässä kanava varataan lähetyksien ajaksi. Kanavan varaus purkautuu erikseen määritellyn aktiivisuusaikaviiveen umpeuduttua. [8]

2.1.2 Fyysinen taso

TETRA-tukiasemat liikennöivät kantoaalloilla, jotka muodostuvat 10 MHz:n taajuusvälillä toimivasta taajuusparista (uplink ja downlink). TETRA-standardin käyttämä TDMA-tekniikka (Time Division Multiple Access) sisältää neljä liikennöintikanavaa yhdessä 25 kHz:n kehyksessä. Yhden aikavälin maksiminopeus datasiirrossa on 7,3 kbit/s, mutta yhdistämällä kaikki neljä kanavaa saadaan siirtonopeudeksi 28,8 kbit/s. Kanavat jaetaan TDMA-kehyksessä liikenne- ja kontrollikanaviin. [8; 20; 22]

TETRA-verkolle on varattu seuraavat taajuuskaistat:

- 380-400 MHz (Viranomaisten TETRA-verkot)
- 410-430 MHz (kaupalliset TETRA-verkot)
- 450-460 ja 460-470 MHz (tulevaisuuden TETRA-verkot) [20]

TETRA:n kehys muodostuu 510 bitistä, 18 TDMA-kehystä muodostaa ylikehyksen ja 60 ylikehystä hyperkehyksen. Ylikehyksen kehyksissä 1-17 siirretään puhetta tai dataa ja kehys 18 on varattu ohjaustiedon välittämiseen. [20]

2.2 Viranomaisverkko ja sen tietoturvallisuusratkaisut

Viranomaisverkko on TETRA-standardiin pohjautuva digitaalinen radioverkko. Se valmistui Suomeen vuonna 2002, jolloin viimeinen tukiasema valmistui. Tukiasemia on yhteensä 1200. Viranomaisverkon kiinteässä osassa on kolmetoista keskusta, joista kaksi on solmukeskuksia. [41]

2.2.1 Viranomaisverkon palvelut

Viranomaisverkon tarjoamat palvelut ovat:

- Ryhmäliikenne, joka on VIRVE-verkossa tavanomainen avoin kanava. Siihen voi osallistua valitsemalla ryhmäpuhelun. Järjestelmä pitää huolen siitä, että vain yksi käyttäjä voi puhua kerrallaan. Yksi käyttäjä voi kuitenkin kuulua useaan eri puheluryhmään. Puheluryhmälle voidaan määritellä toiminta-alue, eikä puheluryhmää voida kuunnella alueen ulkopuolelta.

- Suojattu yksilöpuhelu, joka voi olla kahden päätelaitteen välistä viestintää, päätelaitteen ja hätäkeskuksen välistä viestintää tai kahden hätäkeskuksen välistä viestintää. VIRVE-päätelaitteella pystytään ottamaan myös yhteyttä yleiseen televerkkoon. Keskus ei voi kuunnella yksilöpuheluita.

- Hätäkutsu, joka kuuluu korkeimpaan tärkeysluokitukseen ja se voi keskeyttää muut puhelut tarvitsemaansa kanavakaistaa varten. Hätäkutsulle voidaan ohjelmoida oletuskohde toiseen päätelaitteeseen tai keskukseen.

- Suorakanavatoiminta (DMO), joka muodostetaan kahden päätelaitteen välille. Suorakanavatoiminnassa käytetään suoraa verkkoon kuulumatonta kanavaa, mikä mahdollistaa yhteyden muodostamisen myös verkkoyhteyden puuttuessa. [41]

2.2.2 Tietoturvallisuus

Tietoturvallisuus on käsite, jolla tarkoitetaan tietojen, järjestelmien ja palveluiden suojaamista sekä normaali- että poikkeusoloissa hallinnollisten ja teknisten toimenpiteiden avulla. Tietoturvallisuus rakentuu tiedon kolmen ominaisuuden – luottamuksellisuuden, eheyden ja käytettävyyden – turvaamisesta.

Luottamuksellisuudella tarkoitetaan, että tiedot, järjestelmät ja palvelut ovat vain niihin oikeutettujen saatavissa eikä niitä luvatta paljasteta tai muutoin saateta sivullisten tietoon.

Eheydellä tarkoitetaan, että tiedot, järjestelmät tai palvelut eivät ole laitteisto- ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet.

Käytettävyydellä tarkoitetaan, että tiedot, järjestelmät ja palvelut ovat tarvittaessa niihin oikeutettujen esteettä hyödynnettävissä. [38]

Tässä tutkimuksessa keskitytään luottamuksellisuuden ja käytettävyyden analysointiin. Tällä tutkitaan sivullisten mahdollisuuksia päästä tietoihin käsiksi ja saada pysyvä käytettävyys verkossa tapahtuvaan viestintään.

Viranomaisverkossa toteutetut tietoturvallisuusratkaisut perustuvat kaksitasoiseen salausratkaisuun, jotka ovat:

- Perustaso, jossa on autentikointi eli molemminpuolinen tunnistusmekanismi, sekä ilmarajapinnan salaus, joka on toteutettu radion ja tukiaseman välillä.
- Korkea taso, missä on näiden lisäksi toteutettu päästä päähän -salaus.

[20]

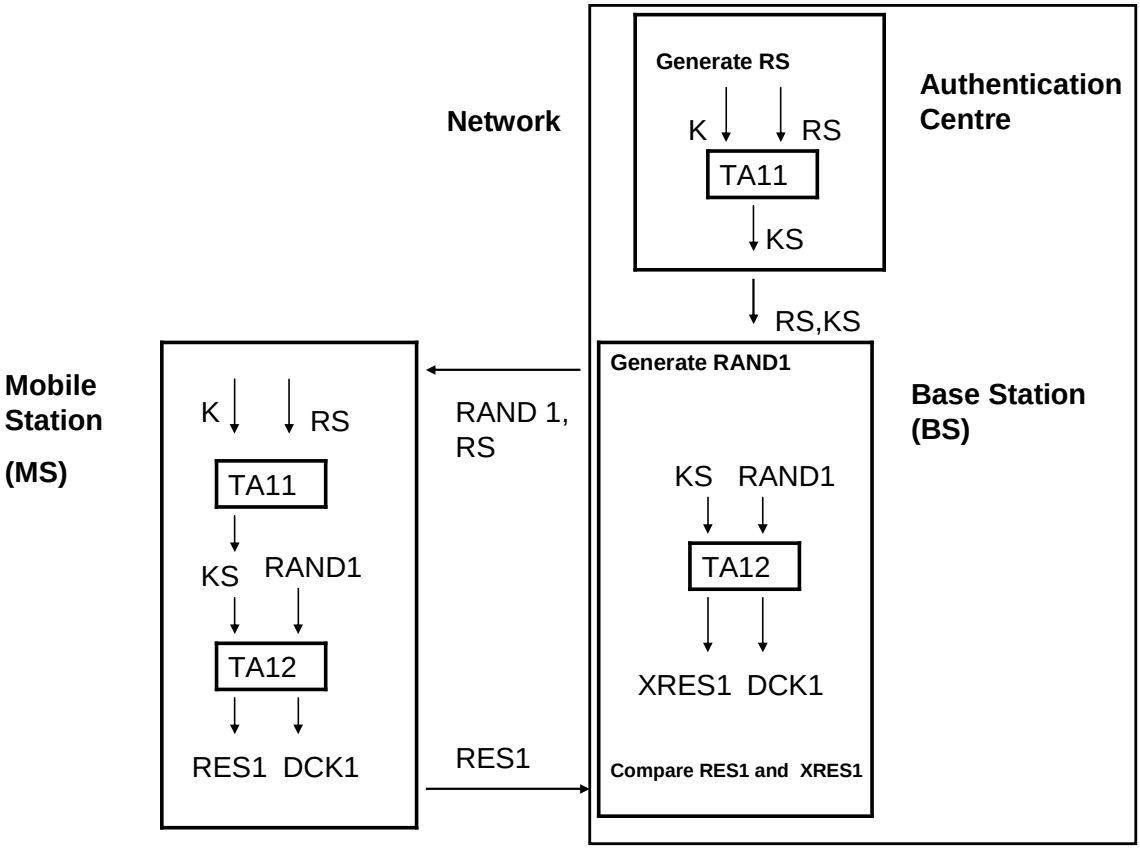
2.2.3 Molemminpuolinen tunnistusmekanismi

Molemminpuolinen tunnistusmekanismi on määritelty TETRA-standardissa. Tunnistusmekanismissa sekä käyttäjä että verkko tunnistavat toisensa. Tunnistusalgoritmeja ei ole rajoitettu standardissa, joten myös yksityisten algoritmien käyttö on mahdollista. Suorakanavarajapintaa varten ei ole käyttäjätunnistusmekanismia, mutta se voidaan toteuttaa epäsuorasti staattista salausavainta käyttäen. [20; 13]

Tunnistusmekanismi perustuu symmetriseen salausavaimeen. Tunnistuksessa osapuolet ovat verkossa sijaitseva tunnistuskeskus ja päätelaite **MS** (Mobile station). **MS** edustaa siihen määriteltyä käyttäjää, eli käytännössä päätelaitteen käyttäjää. Verkko on kaikissa tunnistustapauksissa ohjaava osapuoli. [20]

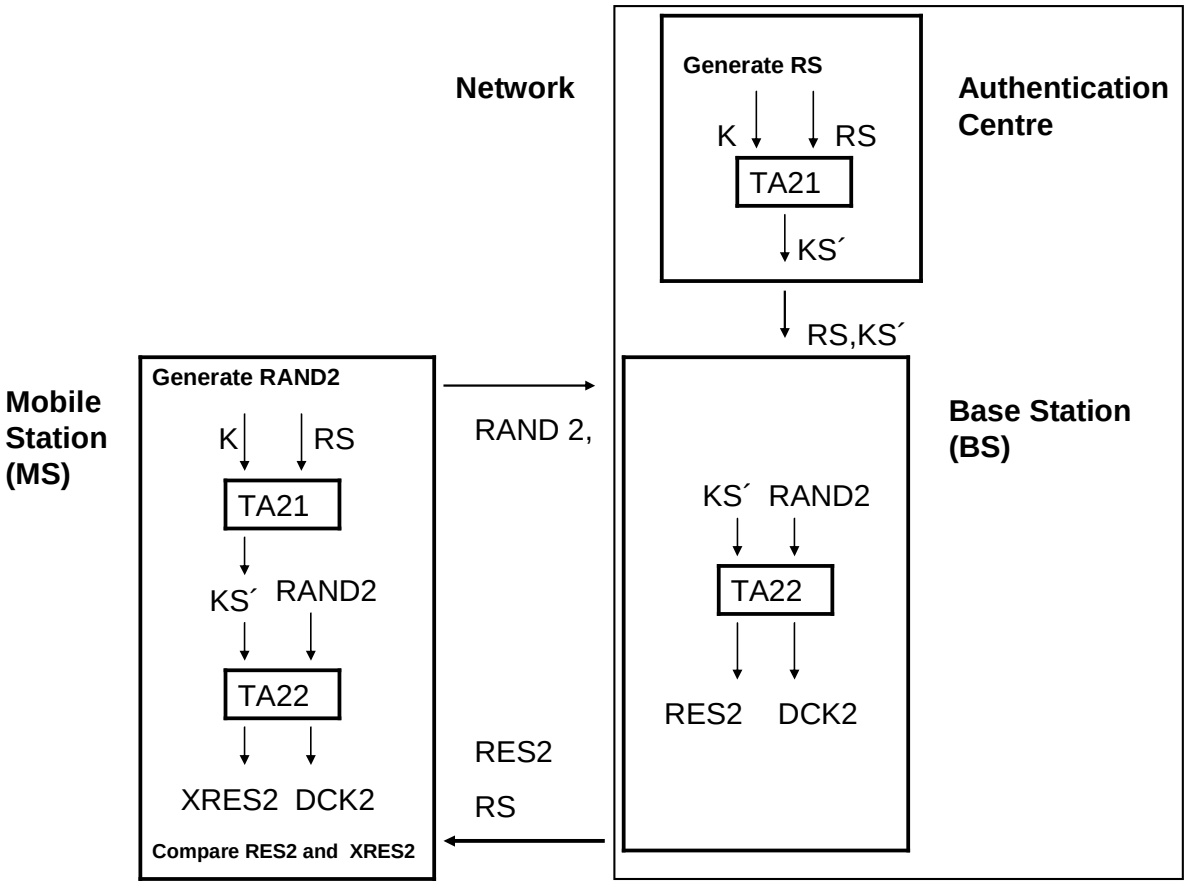
Molemminpuolisessa tunnistuksessa päätöksen tunnistuksen suorittamisesta tekee kutsuttu osapuoli. Tunnistus käynnistyy kutsuvan osapuolen yksipuolisena tunnistuksena, jonka kutsuttu osapuoli muuttaa molemminpuoliseksi tunnistukseksi. Tunnistusprosessi on siis kolmiportainen pyyntö-vastaus-tulos -protokolla. Mikäli ensimmäinen tunnistus epäonnistuu, keskeytyy tunnistusprosessi. Tunnistusprosessin keskeytyessä yhteyttä ei muodosteta. [20]

Kuvassa 1 esitetään esimerkkinä verkon käynnistämä molemminpuolinen tunnistus. Avaimella **K** ja satunnaissiemenluvulla **RS** algoritmin **TA11** kanssa luodaan istuntoon avain **KS**. Verkko lähettää sen jälkeen satunnaisluvun **RAND1** ja satunnaissiemenluvun **RS MS**:lle. **MS** muodostaa istuntoavaimen **KS** käyttäen algoritmia **TA11.** Algoritmia **TA12** käyttäen muodostavat **BS** arvon **XRES1,** sekä **MS** tuloksen **RES1**, jonka **MS** lähettää **BS:**lle vertailua varten. **BS** vertaa saamaansa arvoa **RES1** odotusarvoon **XRES1.** Samalla luodaan avain **DCK1**. [9; 20]



Kuva 1. Molemminpuolinen tunnistus verkon toimesta [9]

Kuvassa 2 esitetään molemminpuolinen tunnistus käyttäjän toimesta. Avaimella **K** ja satunnaissiemenluvulla **RS** algoritmin **TA21** avulla muodostetaan istunnossa käytettävä avain **KS´**. **MS** lähettää satunnaisluvun **RAND2 BS**:lle, joka generoi algoritmin **TA22** avulla tuloksen **RES2** ja avaimen **DCK2**. **BS** lähettää tuloksen **RES2** ja satunnaissiemenluvun **RS MS**:lle, joka avaimen **K**, satunnaissiemenluvun **RS** ja algoritmin **TA21** avulla generoi istuntoavaimen **KS´**. **KS´**:stä ja **RAND2**:sta luodaan algoritmin **TA22** avulla odotusarvo **XRES2** ja avain **DCK2**. [9; 20]



Kuva 2. Molemminpuolinen tunnistus käyttäjän toimesta [9]

Molemminpuolinen tunnistus saadaan yhdistämällä sekä käyttäjän että verkon toteuttamat tunnistukset. Avaimet **DCK1** ja **DCK2** muodostavat yhdistettyinä algoritmin **TB4** avulla molemminpuolisen tunnistuksen tuloksena avaimen **DCK**. [9; 20]

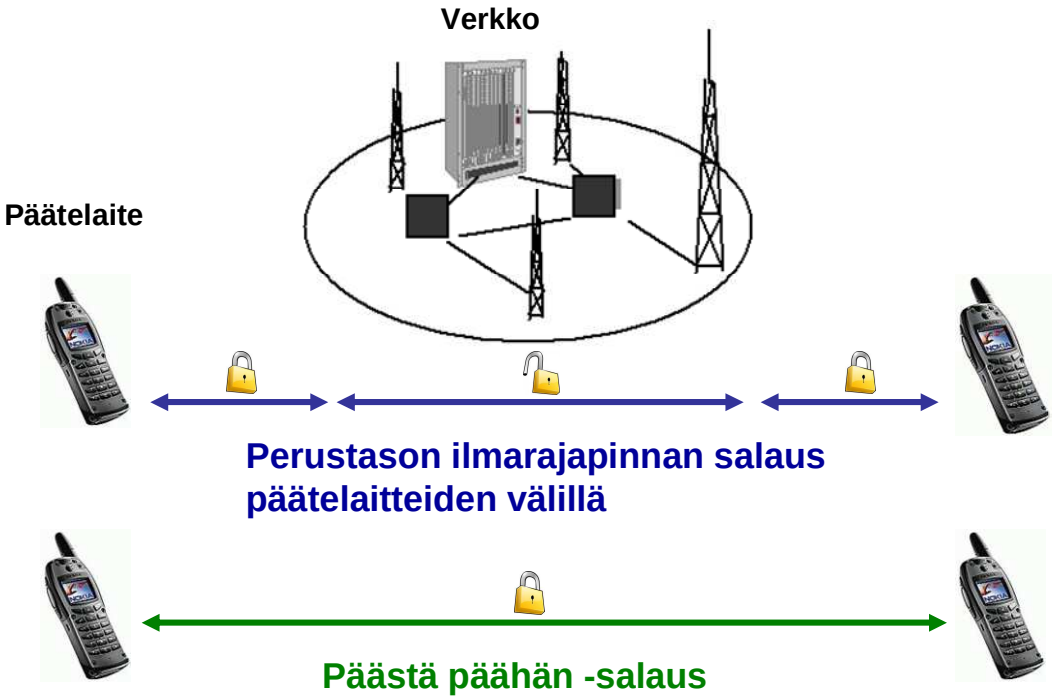
Vieraassa verkossa molemminpuolinen tunnistus voidaan suorittaa kolmella tavalla.

1. lähetetään avain **K** vierailuverkkoon
2. välitetään autentikointivektoreita kotiverkosta vierailuverkkoon
3. välitetään istuntoautentikaatioavain kotiverkosta vierailuverkkoon

TETRA-standardi suosittelee käytettäväksi tapoja kaksi ja kolme. Tapa yksi on näistä huonoin, koska siinä lähetetään kriittinen avain **K**. [41]

2.2.4 Päästä päähän -salaus

Päästä päähän -salaus on tärkeä osa viranomaisverkon korkean tason tietoturvallisuutta. Ilmarajapinnan salaus tarjoaa tietoturvallisen yhteyden käyttäjältä verkkoon. Päästä päähän -salauksessa luodaan vielä turvallisempi yhteys, sillä salattu viesti kulkee salattuna käyttäjältä käyttäjälle. [32] Päästä päähän -salauksen ero ilmarajapinnan salaukseen on selvennetty kuvassa 3. Kuvasta 3 voidaan nähdä, että päästä päähän -salauksessa viesti kulkee verkon läpi salattuna ja luo näin turvallisemman vaihtoehdon. [32]

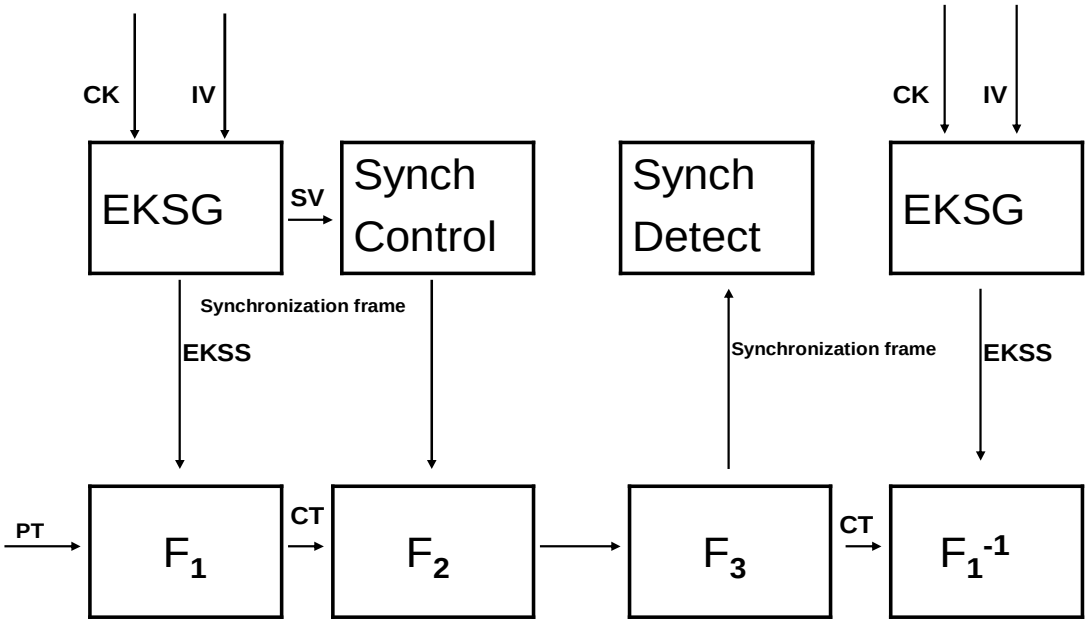


Kuva 3. Päästä päähän -salauksen ero ilmarajapinnan salaukseen [32]

Päästä päähän -salaus on toteutettu TETRA:ssa joustavaksi siten, että siinä ei ole määritelty käytettäviä algoritmeja. Tämä antaa mahdollisuuden käyttäjäorganisaatiolle luoda tarvitsemansa tietoturvataso päästä päähän -salauksella. Puheen salaukselle on TETRA-standardissa määritelty käytettävä rajapinta päästä päähän -salauksessa. Standardi määrittelee myös mekanismin salausjärjestelmän synkronointia varten käytettäessä synkronista jonosalausta. [20]

Kuvassa 4 on esitelty synkroniseen jonosalaukseen perustuva periaate puheen päästä päähän -salauksessa. Salausyksikkö **EKSG** (End-to-end Key Stream Generator) omaa kaksi sisääntu-

loa: salausavaimen **CK** ja alkuarvon **IV** (Initialization Value). Alkuarvo on aikariippuvainen parametri, kuten esimerkiksi aikaleima. Sitä käytetään alustamaan salausyksikön synkronisointi. **EKGS**:n ulostulo on avainjonosegmentti **EKSS** (End-to-end Key Stream Segment). Funktio $\mathbf{F_1}$ yhdistää **PT**:n (Plain Text) bittijonon ja **EKSS**:n tuloksena **CT**:n (Ciper Text) bittijonon. $\mathbf{F_2}$ korvaa puolikkaan aikavälin salatusta bittijonosta synkronointikehyksellä, jonka tuottaa Synch Control. $\mathbf{F_3}$ tunnistaa synkronointikehyksen salatusta bittijonosta ja purkaa sen Synch Detec yksikössä. Funktio $\mathbf{F_1^{-1}}$ purkaa salatun bittijonon selväkieliseksi bittijonoksi.



Kuva 4. Päästä päähän -salauksen jonosalauksen periaate [20]

2.3 Avaimet

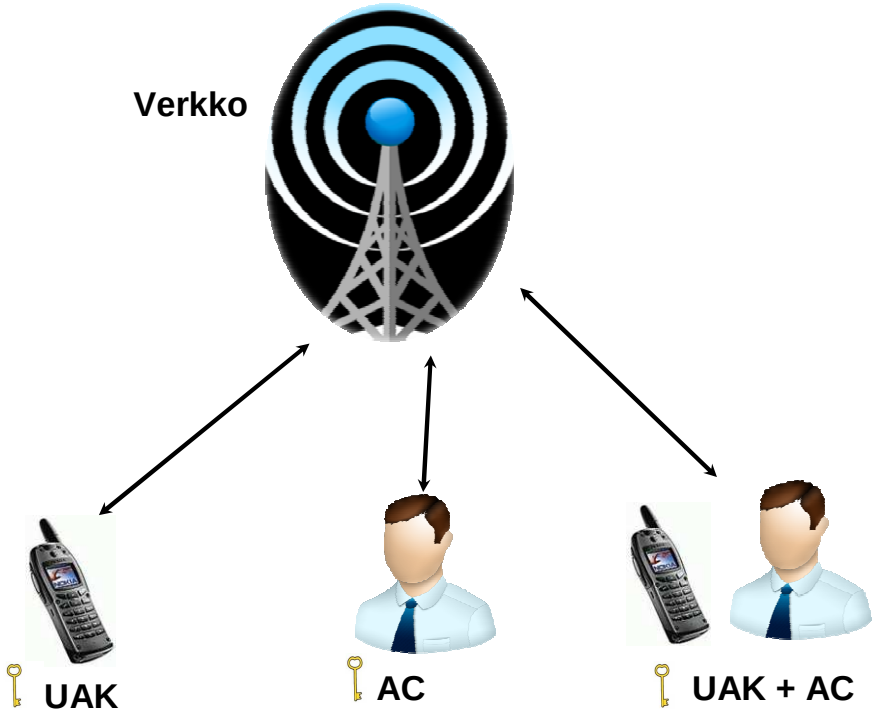
Viranomaisverkossa käytettävät avaimet ovat keskeisiä tietoturvallisuuden ylläpitämiseksi. Avaimilla varmistetaan kaksisuuntainen tunnistus sekä tiedon salaaminen ilmarajapinnassa. Avaimien joutuminen sivullisten käsiin johtaisi VIRVE-verkon luottamuksellisuuden täydelliseen katoamiseen. Avaimet ovat tästä syystä tämän tutkimuksen kannalta yksi merkittävimmistä asioista.

VIRVE-verkon avaimet ovat TETRA-standardin määrittelemiä, ja niitä käytetään eri tilanteissa signaloinnin ja käyttäjäinformaation salausta varten. Standardin määrittelemät avaimet ovat:

- Verkon ja päätelaitteen tunnistukseen käytettävä avain **K. K** voidaan generoida kolmella eri tavalla:

1. Avain luodaan **UAK** (User Authentication Key) avulla, joka on tallennettuna SIM-kortilla tai päätelaitteeseen. Tällöin pystytään tunnistamaan päätelaite.
2. Avain luodaan **AC** (Authentication Code) avulla, joka on käyttäjän henkilökohtainen todennuskoodi. Tällöin tunnistetaan käyttäjä.
3. Avain luodaan käyttämällä **UAK**:tä ja **AC:**ia, jolloin pystytään tunnistamaan sekä laite että käyttäjä. [9; 20; 41]

Kuvassa 5 on havainnollistettu avainten käytön vaikutusta päätelaitteen ja käyttäjän tunnistukseen.



Kuva 5. Avaimen K generoinnin vaikutus käyttäjän tunnistukseen

TETRA-standardin avaimet ilmarajapinnassa ovat:

1. **DCK** (Derived Cipher Key), joka synnytetään autentikaation aikana. **DCK** muodostetaan **DCK1** ja **DCK2**:sta **TB4** algoritmin avulla. Sitä käytetään yhden käyttäjän ja tukiaseman väliseen salaukseen. [9; 20; 41]
2. **CCK** (Common Cipher Key) luodaan verkossa ja salataan **DCK**:lla, minkä jälkeen se lähetetään päätelaitteelle. **CCK**:ta käytetään kaiken ryhmäliikenteen salaukseen yhdellä sijaintialueella. [9; 20; 41]
3. **GCK** (Group Cipher Key) luodaan keskuksessa ja lähetetään tyypillisesti **DCK**:lla salattuna tietylle käyttäjäryhmälle. Avainta voi käyttää sellaisenaan, mutta tyypillisesti

siitä muodostetaan modifioitu versio **MGCK** (Modified Group Cipher Key) sijainti-alueen **CCK**:n avulla. [9; 20; 41]

4. **SCK** (Static Cipher Key) on avain, joka on määrätty etukäteen ja se on voimassa, kunnes se korvataan uudella. Sitä kutsutaan staattiseksi, koska sitä ei muuteta tunnistus-prosessin yhteydessä. TETRA-standardi tukee 32 erilaisen **SCK**:n käyttöä. Avainten valinnat tekee tyypillisesti järjestelmän ylläpitäjä. **SCK**:ta käytetään tyypillisesti **DMO**-puhelujen salaamiseen ja tilanteissa, joissa ei ole käytössä yhteistä **CCK**- tai **GCK**-avainta. Jälkimmäinen tilanne syntyy yleensä puheluissa maantieteellisen rajan yli. [9; 20; 41]

Taulukko 1. Avainten pituudet [7; 20]

80-bittiä	CCK	DCK	SCK	GCK
128-bittiä	K	KS´	KSO	UAK

Avaimet voidaan jakaa liikennöintiin ja signalointiin, ja niiden pituus on 80-bittiä ja näiden avaimien generointiin käytettäviin avaimiin, joiden pituus on 128-bittiä. [20] Käyttäjän tunnistukseen käytettävän PIN-koodin (Personal Identification Number) pituus on 16–32-bittiä. [10]

2.3.1 Avainten hallinta ilmarajapinnassa

Avainten jakamiseksi ja päivittämiseksi on määritelty TETRA:ssa protokolla **OTAR** (Over The Air Re-Keying). Se mahdollistaa avainten **CCK**, **GCK** ja **SCK** turvallisen päivityksen ilmateitse [7; 20]. **OTAR**:ia voidaan hyödyntää myös päästä päähän -salausavaimille [41].

Avaimien luominen on esitelty edellisessä luvussa. Avaimen **CCK** käyttöönottaminen **OTAR**-protokollaa käyttäen toimii siten, että **MS** lähettää tavallisen tunnistuspyynnön ja **CCK**-pyynnön verkolle, joka tunnistusprosessin aikana luo istuntoavaimen **DCK**. Tämän jälkeen avain **CCK** salataan **DCK**:lla ja lähetetään ilmarajapinnan yli **MS**:lle. Prosessi on avaimella **GCK** samankaltainen. [9]

Avain **SCK** lähetetään suoraan päätelaitteeseen käyttäen algoritmeja **TA51** ja **TA52**, joilla muodostetaan käyttäjäkohtainen istuntoavain **KSO**, jolla avain **SCK** suojataan. Päätelaite purkaa salauksen käyttämällä avainta **K** ja satunnaissiemenlukua **RSO** algoritmin **TA41** kanssa. [20]

2.4 Algoritmit

TETRA:ssa käytettävien algoritmien käyttö on tehty joustavaksi. Standardi mahdollistaa yksityisten avaimien käytön kaikissa salausmuodoissa. Ilmarajapinnan salauksen määrittelee ETSI Security Algorithm Group of Experts. Standardiin on määritelty neljä algoritmijoukkoa:

1. TEA 1, joka on tarkoitettu yleiseen käyttöön
2. TEA 2, joka on Schengen-maiden viranomaisten käyttöön tarkoitettu algoritmi. Algoritmi on 80-bittinen.
3. TEA 3, joka on muiden viranomaisten käyttöön tarkoitettu algoritmi. Algoritmi on 80-bittinen.
4. TEA 4, joka on heikennetty algoritmi, jota voidaan käyttää verkoissa, joissa ei ole vahvan salauksen vientilupamenettelyjä. [20; 32]

3 SALAUKSEN JA TUNNISTUKSEN KESTÄVYYS

Tässä luvussa analysoidaan viranomaisverkon salauksen ja tunnistuksen kestävyyttä. Kappaleessa tarkastellaan salauksien kestävyyttä avaimienpituuksien ja algoritmien kestävyyden näkökulmasta. Molemminpuolinen tunnistusmekanismi tarkastellaan sitä vastaan kohdistuvien hyökkäysten näkökulmasta, sekä TETRA:n kykyä kestää näitä. Tunnistusmekanismin lisäksi tarkastellaan käyttäjätunnistuksen luotettavuutta.

3.1 Salauksen purkaminen

Ensimmäisessä kappaleessa käsitellään raa´an voiman hyökkäys eli brute force (väsytysmenetelmä), joka on kaikista salauksen purkamiskeinoista työläin mutta varmin. Toisessa kappaleessa tarkastellaan algoritmien kestävyyttä teoreettisesti. Algoritmien salaisuuden vuoksi tässä tutkimuksessa ei voida tarkemmin tutkia viranomaisverkossa käytettäviä algoritmeja. Kappaleessa esitellään ETSI:n suosittelemaa algoritmia TETRA-standardille päästä päähän -salauksessa, jonka oletetaan tässä tutkimuksessa vastaavan vahvuudeltaan käytettävää algoritmia. Kestävyyttä ja luotettavuutta tarkastellaan esittelemällä todennäköisimmät keinot ja menetelmät, joilla algoritmia vastaan tullaan hyökkäämään. Lisäksi kappaleessa vertaillaan julkisen ja julkaisemattoman algoritmin vahvuuksia ja heikkouksia. Lopuksi tarkastellaan salauksen kestävyyttä tulevaisuudessa ja mahdollisia parannuksia viranomaisverkon tietoturvallisuuteen.

3.1.1 Salauksen purkaminen brute force -menetelmällä

Brute force -attack tai niin sanottu väsytysmenetelmä on salasanojen ja avaimien murtomenetelmä. Se on toiminnaltaan hyvin yksinkertainen, siinä tietokone käy kaikki mahdolliset salasanamahdollisuudet läpi. Vaikka toiminto on työläs, on sen hyvänä puolena sen varma onnistuminen. Mooren lain mukaan tietokoneiden laskentateho kasvaa käytännössä kaksinkertaiseksi 1,5 vuodessa, mikä muuttaa brute force -menetelmän jatkuvasti tehokkaammaksi keinoksi. [16; 30] Brute forcea vastaan ei pysty suojautumaan kokonaan. Salausalgoritmin tulee olla niin varma, että brute force tulee liian kalliiksi ajallisesti ja rahallisesti. Tietokoneiden laskentakapasiteetti määrittää brute forcen käytettävyyden. Laskentatehoa pystytään ostamaan käytännössä rajattomasti. Keskeiseksi kysymykseksi nouseekin brute force -hyökkäystä käytettäessä: Onko tarvittavan laskentatehon ostaminen liian kallista? [4; 17; 21]

Tietokoneen laskentateho muodostuu useasta eri tekijästä, jotka eivät kuitenkaan ole tämän tutkimuksen kannalta merkittäviä. Olennaista brute forcea käytettäessä on maksimaalinen las-

kentateho, joka ilmoitetaan FLOPS:eina (floating point operations per second). FLOPS kertoo yksittäisten laskutoimitusten määrästä sekunnissa [25]. Tätä arvoa käyttäen pystytään vertailemaan tietokoneiden suorituskykyä brute forcea käytettäessä ja pystytään arvioimaan avaimien pituuksien riittävyyttä.

Murtoa pystytään nopeuttamaan myös jakamalla laskentatehtävä usealle tietokoneelle. Tässä menetelmässä kukin tietokone käy läpi sille annetun osan avaimista. Tehtävän järjestelmällisen luonteen vuoksi työn jakaminen on mahdollista ja suoraviivaista. Esimerkiksi 100 koneen käyttö pudottaa murtoajan yhteen sadasosaan alkuperäisestä. [16] Tätä ominaisuutta käytetään hyväksi myös nykyään käytettävissä laskentapilvissä. Taulukossa 2 käytetty laskentapilvi on kaupallisen yhtiön tarjoamaa laskentatehoa. [7]

Brute force -hyökkäyksen avainavaruuden laskemiseksi käytetään kaavaa 2^n, jossa n on avaimen pituus. [17] Taulukossa 2 vertaillaan kahden eri avainpituuden kestävyyttä eri tehoisia tietokoneita vastaan. Taulukosta käy ilmi avaimen pituuden merkitys. Avaimen pituuden kasvaessa kaksinkertaistuu avainavaruus, mikä kaksinkertaistaa brute forcen työmäärän. [4; 17] Alla olevia tuloksia tarkasteltaessa tulee ottaa huomioon se, että kyseessä olevat arvot ovat viitteellisiä. Laskentatehot ovat teoreettisia huippuja ja laskentaan kuluva aika on maksimaalinen. Todennäköistä on, että avain ei löydy viimeisellä yrityksellä. Taulukon laskutoimitukset löytyvät liitteestä 1.

Taulukko 2. Tietokoneiden laskentateho ja avaimien murtamiseen kuluva aika.

Tietokone malli	Flopsien määrä/Laskentateho	Kuluva aika 64-bittiseen avaimeen	Kuluva aika 80-bittiseen avaimeen
Pentium4 + SSE3, 3.6GHz (tavallinen tietokone)	7.2 GFlops [6]	n. 80 vuotta	n. 50 miljoonaa vuotta
Laskentapilvi (Amazon)	1 Teraflop [3]	n. 214 vuorokautta	n. 38 tuhatta vuotta
Supertietokone	16 petaflops [5]	n. 20 minuuttia	n. 2,4 vuotta

Brute forcen kannattavuuden tutkimiseksi tulee tarkastella menetelmän hintaa. Laskentatehon hinnat ovat kehittyneet käytännössä Mooren lain mukana [16; 17]. Taulukossa 3 on laskettu arvio kolmen eri salasananmurtamiseen kuluvista kustannuksista nykyisillä hinnoilla kotikonstein rakennettavilla menetelmillä. Laskenta on suoritettu siten, että murtamiseen menee noin sekunti, ja että salasana murtuu vasta viimeisellä yrityksellä.

Taulukko 3. Salasanan murtamisen hinta, kun 1 TERAFLOPS:ia maksaa 232,60€. [2; 35]

40 bit	$2^{40} / 10^{12} * 232,6€ = \sim 256$ €
64 bit	$2^{64} / 10^{12} * 232,6€ = \sim 4.290$ miljardia €
80 bit	$2^{80} / 10^{12} * 232,6€ = \sim 280$ biljoonaa €

3.1.2 Algoritmien kestävyys ja luotettavuus

TETRA-standardi tukee kaksitasoista tietoturvaa. Tietoturva jaetaan perustasoon, joka käsittää ilmarajapinnan turvaamisen GSM-tasoisella salauksella ja ylempään tasoon, eli puheen ja datan päästä päähän -salaukseen, jonka avulla TETRA-liikennettä voidaan välittää muissa verkoissa [22].

Kerckhoffin periaatteen mukaan salausjärjestelmä on varma, jos siitä voidaan julkaista kaikki sen salaus- ja purkuprosessien yksityiskohdat lukuun ottamatta salaista avainta [17]. Viranomaisverkon käyttämät algoritmit ovat salaisia [20]. Salaisen algoritmin luotettavuus on kyseenalainen Kerchoffin periaatteen mukaan [17]. Sotilaskäytössä salattujen algoritmien käyttäminen on yleistä. Salatun algoritmin käyttämisen etuna on, että algoritmia vastaan ei voida hyökätä ennen kuin se on takaisinmallinnettu eli itse algoritmi on selvitetty. Takaisinmallintamisessa algoritmi päätellään sen tuottaman datan avulla. Takaisinmallintaminen on työläs prosessi, joka vie aikaa ja rahaa. Takaisinmallintamisen kustannukset ovat arviolta noin kymmenentuhannen ja miljoonan euron välillä algoritmia kohden. [18]

Salattu algoritmi ei välttämättä ole heikko, vaikka Kerckhoffin periaatteen mukaan se ei ole varma. Täysin omatekemät algoritmit, jotka eivät ole olleet julkisesti analysoitavissa, ovat usein heikkoja. Mahdollista on kuitenkin tehdä tunnetun algoritmin päälle algoritmi. Näin al-

goritmi on erilainen kuin tunnettu algoritmi, mutta oikein tehtynä se on vähintään yhtä turvallinen. [18]

TETRA:n käyttämää TEA-algoritmia vastaan hyökätessä tulee ensin tarkastella, mitä algoritmista tiedetään, jotta algoritmia voidaan analysoida ja etsiä siitä heikkouksia. Käytettävästä algoritmista tiedetään, että sen avaimenpituus on 80 bittiä. 80 bitin avain antaa viitteitä siitä, että se on vanha algoritmi. Tämän enempää algoritmista ei voida ilman takaisinmallintamista päätellä. Lisäksi myös avaimen pituuden perusteella vanhaksi arviointi on käytännössä arvailua. [18]

TEA-algoritmia ja muita salaisia algoritmeja vastaan voidaan hyökätä Cube-hyökkäyksellä [18]. Cube-hyökkäys on Itai Dinurin ja Adi Shamirin vuonna 2008 kehittämä uusi yleinen tapa hyökätä algoritmeja vastaan. Sen käytettävyydestä he kirjoittavat pro gradussaan seuraavasti: ”They can be applied to any cryptosystem that takes secret and public inputs to produce an attack that derives the secret input [24]. ” Vapaasti suomennettuna tämä tarkoittaa: Sitä pystyy soveltamaan jokaiseen salausjärjestelmään, joka käyttää salaista ja julkista dataa muodostaen tästä hyökkäyksen, josta johdetaan salainen data.
Cube-hyökkäys ei tarvitse onnistuakseen minkäänlaista tietoa algoritmista tai salausjärjestelmästä. Salausjärjestelmää voidaan kohdella kuten ”mustaa laatikkoa” [24].

Päästä päähän -salauksessa ETSI suosittelee käytettäväksi IDEA-algoritmia (International Data Encryption Standart) [32]. IDEA-algoritmin toimintaperiaate on seuraava: Salaus aloitetaan jakamalla 64 bitin selväkielilohkot 16 bitin alilohkoiksi. Kuhunkin alkiolohkoon kohdistetaan laskentaiteraatioita, joihin osallistuu 52 erilaista 128 bitin avaimesta muodostettua aliavainta. Iteraatiokierroksia on yhteensä 8. Kunkin iteraatiokierroksen laskenta on yksinkertaista bitti bitiltä toteutettua mod 2-yhteenlaskua. Viimeisen kierroksen jälkeen neljä alilohkoa liitetään yhteen, mistä muodostuu 64 bitin salattu lohko. [17]

IDEA-algoritmista ei ole tullut julkisuuteen murtautumismenetelmää. Brute force on näin ollen ainoa toimiva tapa hyökätä sitä vastaan. 128 bitin avaimen murtaminen brute forcella, kun käytössä on 10^9 tietokonetta, jotka laskevat 10^9 laskutoimitusta sekunnissa, kestäisi noin tuhat kertaa universumin iän verran. [17]

Mahdollisesti toimiva tapa IDEAn murtamiseen on selvittää peräkkäisten selväkielilohkojen ja niitä vastaavien salasanomalohkojen välistä statistista riippuvuutta algoritmin sisäisestä ra-

kenteesta. Ongelmaksi tässä kehkeytyy IDEAn monipuolinen ja monimutkainen tapa käyttää aritmeettisia ja epälineaarisia laskutoimituksia, mikä tekee tästäkin murtamistavasta heikon. [17]

3.1.3 Salauksen kestävyys tulevaisuudessa

Tulevaisuudessa 80 bitin salausavaimen pituus on liian lyhyt. 80 bitin avain kestää vielä teoriassa murtamisen nykytietotekniikalla, mutta esimerkiksi valtiohallinnon tietoturvallisuuden johtoryhmä ei pidä 80 bitin avainta riittävän vahvana. [37] Tietokoneiden laskentatehon kasvun oletetaan etenevän Mooren lain mukaan, mikä tarkoittaa sitä, että avaimen pituuden tulisi kasvaa samassa tahdissa laskentatehoon nähden. Tämä tarkoittaisi yhden bitin lisäämistä avainpituuteen vähintään seitsemän vuoden välein [16].

IDEA kestää 128 bitin avaimenpituudellaan nykyteknologian mukaisia murtoja vielä vuosikymmeniä. Kuten osiosta 3.2 käy esille, se on brute forcea käytettäessä käytännössä murtamaton vielä hyvinkin pitkään. Teknologia ja kryptoanalyysi voivat kuitenkin kehittyä tulevina vuosikymmeninä aivan uudelle tasolle, mutta toisaalta fysiikan asettamat rajoitukset saattavat olla myös estämässä prosessointitehon jatkuvaa kasvua. [17]

Teknologia, joka mullistaa varmasti lähes kaikki käytössä olevat salausjärjestelmät, on kvanttitietokone. Tämä vain 300 atomin kokoinen tietokone pystyy tekemään enemmän laskutoimituksia kuin maailmankaikkeutta suurempi nykytekniikalla toimiva supertietokone. Se kykenee 10^{75}–10^{80} kertaa supertietokoneita tehokkaampaan laskentaan [26; 34].

Kvanttitietokoneen ylivertaisuus nykyaikaisiin tietokoneisiin perustuu sen kyvystä laskea useampaa laskutoimitusta yhtä aikaa. [34] Kvanttitietokoneen valmistumiseen arvioidaan kuluvan vielä noin 10–15 vuotta [19].

Tulevaisuudessa tietoturvallisuuden romahtamisen mahdollisena syynä voi olla myös tietovuoto. Viranomaisverkossa käytettävät algoritmit ovat salaisia, minkä vuoksi niiden heikkouksia ei ole mahdollisesti tutkittu tarpeeksi [17; 20]. Heikkouden tai algoritmin vuotaminen julkisuuteen, kuten GSM-verkolle tapahtui, heikentää tietoturvallisuutta [42].

Takaovi-ohjelma (back door) on myös mahdollinen tietoturvariski. Takaovella tarkoitetaan porttia, jonka avulla alkuperäinen tekijä pystyy ohittamaan kaikki suojaukset. Takaovia usko-

taan olevan ainakin suurvaltojen myymissä asejärjestelmissä, joiden avulla ne pystyvät lamauttamaan järjestelmät tarvittaessa [16].

Viranomaisverkon tietoturvapuutteita tutkitaan aktiivisesti. Viestintäviraston mukaan päästä päähän -salauksen käyttäminen TETRA-päätelaitteiden välillä on tämän vuoksi tärkeää [43]. Tietoturvallisuutta parantava päivitys olisi IDEA-algoritmin vaihtaminen esimerkiksi AES-algoritmiin, jossa lohkokoko on suurempi. [18; 33]

3.2 Molemminpuolisen tunnistusmekanismin kestävyys

Tässä luvussa esitellyt hyökkäykset ovat teoreettisia, eikä niiden toimivuutta ole tässä tutkielmassa todennettu. Oletettavaa kuitenkin on, että mikäli molemminpuolista tunnistusmekanismia vastaan hyökätään, tulevat hyökkäykset noudattamaan samoja periaatteita.

3.2.1 Molemminpuoliseen tunnistusmekanismiin kohdistuvat mahdolliset hyökkäykset

Molemminpuolista tunnistusmekanismia vastaan kohdistuvat hyökkäykset jakautuvat karkeasti kahteen kategoriaan:

1. verkon suorittamaa, käyttäjän ja mobiililaitteen tunnistusta vastaan
2. hyökkäys käyttäjän ja mobiililaitteen verkontunnistusta vastaan.

Suurimman uhkan tunnistukselle aiheuttavat kuitenkin varastetut ja laittomasti haltuun otetut mobiililaitteet, joiden avulla hyökkääjä pystyy salakuuntelemaan verkkoa vaivattomasti. [1]

Varastettujen ja kadonneiden päätelaitteiden lisäksi voidaan tunnistusprosessia vastaan hyökätä myös kloonaamalla päätelaite. Tunnistuksessa käytetään kryptografista todennusta. Todennuksen vahvuuden määrittää käytettävä algoritmi. Heikko algoritmi aiheuttaa uhkan, koska se mahdollistaa SIM-kortille tai mobiililaitteeseen tallennetun salaisen datan paljastumisen, jotka sisältävät muun muassa tunnistuksen ja kloonauksen kannalta kriittiset parametrit. [1] Tunnistukseen käytettävät algoritmit ja avaimet on esitelty luvussa 2.3 ja algoritmien kestävyys luvussa 3.1.2 Mikäli hyökkääjä saa käsiinsä oikeat parametrit, pystyy se kloonaamaan päätelaitteen, jonka pääsyä verkkoon ei voida estää [28].

3.2.2 Molemminpuolisen tunnistusmekanismin ominaisuudet hyökkäyksiä vastaan

TETRA:n molemminpuolisen tunnistusmekanismin ansioista varastetut tai kopioidut päätelaitteet eivät pysty salakuuntelemaan verkkoa. Kuten luvussa 2.3 käy ilmi, muodostetaan tunnistusavain **K** siten, että verkko tunnistaa joko käyttäjän, päätelaitteen tai molemmat. [14; 20] TETRA:n tietoturvaominaisuuksiin kuuluu kyky yksittäisten päätelaitteiden väliaikaiseen tai pysyvään poiskytkentään verkosta. Päätelaite voidaan kytkeä pois verkosta esimerkiksi huollon ajaksi, katoamisen tai varkauden vuoksi. Väliaikainen poiskytkentä voidaan tehdä langattomasti. Poiskytkentä estää päätelaitteen yksilöllisen tunnistenumeron käytön verkon laitteissa, jolloin kyseisellä päätelaiteella ei voi käyttää verkon palveluja. Päätelaite pysyy kuitenkin rekisteröitynä verkkoon, ja se voidaan haluttaessa palauttaa käyttökelpoiseksi. Päätelaitteen pysyvä poiskytkentä on myös mahdollista tehdä langattomasti verkon kautta, mikä tekee koko laitteen pysyvästi toimintakyvyttömäksi. Ainoa keino palauttaa pysyvästi poiskytketty päätelaite on toimittaa se laitevalmistajalle uudelleenkytkentää varten. [20; 23]

Päätelaitteen kloonaaminen on Yong-Seok Parkin, Choon-Soo Kimin ja Jae-Cheol Ryouin tekemän kokeen mukaan mahdollista. Kloonauksen onnistuminen vaatii avaimen **K** ja yksilöllisen tunnistenumeron **ISSI** (Individual Short Subscriber Identity). **ISSI** muodostetaan vähentämällä 10-bittinen maatunnus **TMCC** (TETRA Mobile Country Code) ja 14-bittinen verkkotunnus **TMNC** (TETRA Mobile Network Code) TETRA:n tilaajatunnuksista **ITSI** (Individual Tetra Subscriber Identities), jotka ovat laitekohtaisia. **ISSI**-koodin ja avaimen **K** avulla pystytään luomaan onnistuneesti kloonattu päätelaite. [28; 31]

Suorakanavarajapinnassa heikkoutena on tunnistusmekanismin puuttuminen. Mekanismin puuttuminen voidaan kuitenkin epäsuorasti korvata käyttämällä avainta **SCK** (static cipher key) [20].

3.3 Käyttäjien tunnistamisen luotettavuus

Molemminpuolisessa tunnistusmekanismissa päätelaite tunnistetaan SIM-kortille tallennettujen algoritmien ja parametrien avulla [11]. Algoritmit ja tunnistusmekanismi on esitelty luvussa 2.2.3. SIM-kortti on kriittinen käyttäjän tunnistuksen kannalta sen sisältävän datan vuoksi. Tärkeän datan vuoksi sen tulisi olla riittävän hyvin salattu, jotta hyökkääjä ei pääse sen sisältöön käsiksi ja käyttäjätunnistus pysyisi luotettavana. TETRA:ssa käyttäjä tunnistetaan hänen henkilökohtaisen PIN-koodinsa (Personal Identification Number) avulla. TETRA-standardissa

PIN-koodin pituus on 16–32 bittiä. Kuten luvusta 3.1.1 käy ilmi, on tämän pituisen avaimen murtaminen brute forcella mahdollista jo perustietokoneella.

Tunnistusta voidaan pitää valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) laatiman ohjeen mukaan heikkona, koska siinä vaaditaan ainoastaan salasana. Vahva tunnistaminen vaatisi VAHTI:n mukaan kaksiosaista tunnistamista. TETRA:n tapauksessa se voisi olla varmenteellinen sirukortti ja PIN-koodi. [39]

4 JOHTOPÄÄTÖKSET

Viranomaisverkon tietoturva perustuu kahteen tietoturvatasoon, perustasoon ja ylempään tasoon. Näillä estetään viranomaisverkon salakuuntelu. Perustaso on ilmarajapinnan salaamiseen tarkoitettu taso, joka on salattu salaista algoritmia käyttäen 80-bittisellä avaimella. Ylempi taso on päästä päähän -salaus, joka on suojattu 128-bittisellä avaimella ja tunnetulla algoritmilla, jonka tässä tutkimuksessa oletetaan olevan ETSI:n suosittelema IDEA-algoritmi.

Kuten edellisissä luvuissa käy ilmi, on perustason ilmarajapinnan salaus liian heikko. Ilmarajapinnan 80-bittisen avaimen tuoma tietoturvallisuus on heikko jo brute forcea käytettäessä. Sen murtaminen onnistuu brute forcea käyttäen jo nykytekniikalla, mikä osoittaa sen riittämättömyyden nyt ja varsinkin lähitulevaisuudessa. Ilmarajapinnan salauksessa käytettävää algoritmia ei tässä tutkimuksessa pystytty tarkastelemaan sen salaisuuden vuoksi, mutta salainen algoritmi herättää yleisesti kysymyksen sen luotettavuudesta. Algoritmin selvittämiseksi tulisi tehdä takaisinmallintaminen, jonka jälkeen algoritmin heikkouksia olisi mahdollista tutkia. Kuten tutkielmassa todetaan, on avaimen **K** merkitys kriittinen tietoturvallisuuden ylläpitämiseksi, sen vuotaminen ulkopuoliselle johtaisi tietoturvallisuuden romahtamiseen.

Molemminpuolinen tunnistusmekanismi on toteutettu TETRA:ssa hyvin. Sen 128-bittinen avaimenluontialgoritmi tekee sen murtamisesta vaikean, myös verkon kontrolloima tunnistusprosessi on toteutettu hyvin. Mahdollisen heikkouden voivat muodostaa kloonatut päätelaitteet, joiden avulla pystytään murtamaan tunnistusmekanismi. TETRA-verkon ominaisuus tunnistaa ja estää varastetut ja kadonneet päätelaitteet mahdollistaa todennäköisesti myös kloonattujen päätelaitteiden estämisen, mutta asian varmistamiseksi se vaatisi jatkotutkimuksia.

Käyttäjän tunnistamiseen liittyvä 16–32-bittinen PIN-koodi on helposti murrettavissa esimerkiksi brute forcella. Brute forcen lisäksi PIN-koodin turvallisuuden kannalta merkittävää on käyttäjän koodin valinta. Yksinkertaiset numeroyhdistelmät ovat helposti murrettavissa jo pelkällä arvaamisella, toisaalta TETRA:n ominaisuus tunnistaa ja kuolettaa päätelaite verkon toimesta tekee varastetuista tai kadonneista päätelaitteista kohdistuvan uhkan pieneksi.

Ei ollut havaittavissa, että ylemmän tason päästä päähän -salauksessa olisi suuria puutteita. IDEA-algoritmi on 128-bittisellä avaimella turvallinen myös lähitulevaisuudessa. Brute forcea käyttäen ei nykytekniikalla pystytä murtamaan 128-bittistä avainta vielä moneen vuosikym-

meneen. Algoritmi on myös kestänyt julkisen vertailun, eikä ole odotettavissa, että se murtuisi lähitulevaisuudessa kryptoanalyysin avulla.

Kuten luvussa 3 todetaan, on viranomaisverkon TETRA-standardin mukaisen salauksen murtaminen hyvin kallista. Brute forcea käyttäen tarvitaan useampi supertietokoneen tasoinen tietokone, mikä nostaa kustannukset todella korkealle. Tästä voidaan päätellä, että brute force murtautumiskeinona on mahdollinen ainoastaan suurilla valtiollisilla tiedustelutoimistoilla kuten esimerkiksi USA:n NSA:lla (National Security Agency) ja Venäläisellä FAPSI:lla (Federal Agency of Goverment Communications and Information). IDEA:n kestävyyden ja TEA-algoritmien salaisuuden vuoksi on myös epätodennäköistä, että pienemmät organisaatiot tai yksittäiset henkilöt kykenisivät murtamaan algoritmit ja kuuntelemaan viranomaisverkkoa. TEA-algoritmien selvittäminen vaatisi takaisinmallinnuksen, mikä on jo itsessään työläs projekti. Takaisinmallinnus ei myöskään takaa algoritmin murtamista, mikä lisää sen tekemisen kynnystä.

Tietoturvallisuuden murtuminen on mahdollista, mikäli tapahtuu TEA-algoritmiin liittyvä tietovuoto. Riski on standardin kansainvälisyyden kannalta merkittävä. Ulkomaisen organisaation suunnittelema standardi jättää myös takaportin mahdollisuuden auki. Takaportista ei löytynyt tutkimusta tehdessä mitään viitteitä, mutta myöskään sitä kieltävää aineistoa ei ollut saatavilla.

Tuloksia voidaan hyödyntää jatkotutkimuksissa kokonaistietoturvan kartoittamisessa. Tutkielma vastaa algoritmien ja avaimenpituuksiin liittyviin tietoturvakysymyksiin ja niihin liittyviin ongelmiin, mutta viranomaisverkon todellisen tietoturvallisuuden tarkasteleminen vaatisi laajempaa analysointia. Jatkotutkimuksia tulisi tehdä päästä päähän -salauksen käytettävyydestä, protokollavirheistä, tietojärjestelmän haavoittuvuudesta, käyttäjävirheistä aiheutuvista tietoturvariskeistä ja verkon rakenteen aiheuttamista tietoturvariskeistä. Kuten lähteistä ilmenee, on algoritmeja vastaan hyökkääminen työläs tapa murtautua verkkoon. Tämän takia olisi hyökkääjällekin edullisempaa yrittää hyökätä tietojärjestelmää tai protokollia vastaan. Käytettävyyden tutkiminen osoittaisi, että salausjärjestelmiä pystytään hyödyntämään. Käytettävyys on merkittävä asia, sillä huono käytettävyys johtaa salausjärjestelmien käytöstä poistamiseen.

Tutkielman perusteella voidaan todeta, että TETRA-standardin mukaisen viranomaisverkon salaus on riittävä päästä päähän -salausta käytettäessä, mutta perustason ilmarajapinnan salaus on sitä vastoin heikompi ja se vaatisi päivityksen, jotta sen luoma tietoturvallisuus olisi luotettava.

LÄHTEET

[1] Ahonen, Pasi & al. *Mobiilimaailman tietoturvauhkat ja ratkaisut*. LUOTI-julkaisuja 1/2005. Helsinki: Luoti. 2005. 97 s. ISBN 952-201-286-6, 952-201-287-4

[2] Amazon. *AMD-Fire Stream TM-9270 computer accelerator.* [viitattu 14.10.2012]. Saatavissa: http://www.amazon.co.uk/AMD-FireStreamTM-9270-Compute-Accelerator/dp/B0021AEQQ6/ref=sr_1_1?ie=UTF8&qid=1350207776&sr=8-1

[3] Bakke, Kurt. *Amazon Offers Teraflop Supercomputing for $2.10 per hour* **.** 2011**.** [viitattu30.9.2012].Saatavissa: http://www.conceivablytech.com/4110/products/amazon-offers-teraflop-supercomputing-for-2-10-per-hour

[4] Bauer, Friedrich. *Decrypted secrets: Methods and Maxims of Cryptology.* 2 Painos. Berliini: Springer-Verlag, 2000. 473 s. ISBN 3-540-42674-4

[5] Brodkin, Jon. *With 16 petaflops and 1,6M cores, DOE supercomputer is world´s fastest.* 2012. [viitattu 14.10.2012]. Saatavissa: http://arstechnica.com/information-technology/2012/06/with-16-petaflops-and-1-6m-cores-doe-supercomputer-is-worlds-fastest/

[6] Chen, Thomas & al. *Cell Broadband Engine Architecture and its first implementation A performance view.* 2005 [viitattu 20.2.2013]. Saatavissa: http://www.ibm.com/developerworks/power/library/pa-cellperf/

[7] Finkle, Jim. *Amazon cloud can help hack WiFi networks:expert.* Reuters [viitattu 7.1.2011]. Saatavissa: http://uk.reuters.com/article/2011/01/07/us-amazon-hacking-idUKTRE70641M20110107

[8] ETR 300-1: *Terrestial Trunked Radio (TETRA); Voice plus Data (V+D); Designers´ guide. Part 1: Overview, technical description and radio aspects*, European standard. 1997. 84 s.

[9] ETSI 3 EN 300 392-7: V 2.1.1. *Terrestrial Trunked Radio (TETRA);Voice plus Data ;Part 7: Security*. European standard. 2001

[10] ETSI 3 EN 300 392-7: V 3.1.1. *Terrestrial Trunked Radio (TETRA);Voice plus Data ;Part 7: Security*. European standard. 2008

[11] ETSI ES 200 812-2: V 2.2.2. *Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 2: Characteristics of the TSIM application.* European standard. 133 s.

[12] ETSI. *About ETSI*. [viitattu 28.9.2012]. Saatavissa: http://www.etsi.org/WebSite/AboutETSI/AboutEtsi.aspx

[13] ETSI EN 300 175-7. V 2.3.1. *Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features.* Ranska: European Standard. 2010. 109 s.

[14] Heikkonen, Kimmo, Pesonen, Tero, Saaristo, Tiina. *You and Your Tetra Radio.* 2 painos. Suomi: Edita Prima Inc. 2004. 97 s. ISBN: 951-826-770-7

[15] Helenius, Paavilainen, Rautiainen et.al, *Tietoturvallisuuden Erityiskysymyksiä 2004*, Seminaarityö. Tampere, 2004. Tampereen yliopisto, Tietojenkäsittelytieteiden laitos, 206 s.

[16] Järvinen, Petteri. *Tietoturva & yksityisyys*. 2 Painos. Porvoo: WS Bookwell. 2002. 456 s. ISBN: 951-846-152-X

[17] Kerttula, Esa. *Tietoverkkojen tietoturva*. 2. uudistettu painos. Helsinki: Oy Edita Ab. 1999. 510 s. ISBN 951-37-2904-4

[18] Kiviharju, Mikko. DI, vanhempi tutkija, Puolustusvoimat. Riihimäki Haastattelu, Algoritmien kestävyys, tutkiminen ja hyökkääminen niitä vastaan, 16.11.2012. Haastattelumuistiinpanot tutkijalla.

[19] Korhonen, Suvi. *Kvanttitietokoneiden tutkimuksessa läpimurto*. 2012. [viitattu 17.11.2012]. Saatavissa: www.tietoviikko.fi/kaikki_uutiset/kvanttitietokoneiden+tutkimuksissa+lapimurto/a784656

[20] Korkiamäki, Ilkka: *TETRA järjestelmän sotilaalliset käyttömahdollisuudet*. Maanpuolustuskorkeakoulu, Tekniikan laitos, Julkaisusarja 1, Tutkimuksia, n:o 9. Helsinki: Oy Edita Ab. 2001.140 s. ISBN 951-25-1217-3

[21] Kosola, Jyri ja Solante, Janne. *Elektroninen sodankäynti, osa 1 – taistelun viides dimensio*. Helsinki: Edita Prima Oy, 2004. 223 s. ISBN 951-25-15554-7

[22] Kosola, Jyri, Solante, Tero. *Digitaalinen taistelukenttä informaatioajan sotakoneen tekniikka*. Julkaisusarja 1. Helsinki: Oy Edita Ab. 2000. 402 s. ISBN 951-25-1143-6

[23] Laakso, Jari, Leino, Hannu-Heikki. *TETRA–radioverkkojärjestelmän turvallisuuden tutkimus teknisen vertailun ja riskianalyysin avulla.* Opinnäytetyö. Leppävaara, 2011. Laurea-ammattikorkeakoulu. 81 s.

[24] Lathrop, Joel: *Cube attacks on cryptographic hash functions*. Pro gradu. Rochester. 2009. Rochester institute of technology, Department of Computer Science. 65 s.

[25] Lehikoinen, Elisa, Parkko, Julia, et al. *Supertietokoneet.* Seminaarityö. Lappeenranta. 2009. Lappeenrannan teknillinen yliopisto. Tietotekniikan osasto. 18 s.

[26] Luotola, Janne. *Uusi kvanttitietokone voi olla jopa 10^80 kertaa tehokkaampi kuin nykyiset supertietokoneet*. Tekniikka & Talous. 2012. [viitattu 17.11.2012]. Saatavissa:

www.tekniikkatalous.fi/innovaatiot/tiede/uusi+kvanttitietokone+voi+olla+jopa+1080+kertaa+tehokkaampi+kuin+nykyiset+supertietokoneet/a803640

[27] Nurminen, Jussi. *Datan siirto viranomaisverkossa*. Kandidaatintutkielma. Helsinki, 2005. Maanpuolustuskorkeakoulu. Tekniikanlaitos, 27 s.

[28] Park. Yong-Seok et al. *The Vulnerability Analysis and Improvement of the TETRA Authentication Protocol* [viitattu 5.3.2013]. Saatavissa: http://www.icact.org/upload/2010/0423/20100423_Abstract_B.pdf

[29] Posti, Anu. *Salausmenetelmät osana elektroniselta tiedustelulta suojautumista*. Kandidaatintutkielma. Helsinki, 2006. Maanpuolustuskorkeakoulu. Tekniikanlaitos, 25 s.

[30] Pyykkönen, Petteri. *2.3 Murtotekniikat.* Oulun kauppaoppilaitos [verkkojulkaisu]. 2004. [viitattu 28.9.2012]. Saatavissa: http://www.okol.org/verkkokurssit/datanomi/tietojarjestelmien_kehittaminen/tietoturvajarjestelmat/internetin_tietoturva/murtotekniikat.htm

[31] *Regeln für die Zuteilung von Individuellen TETRA Teilnehmerkennungen.* 2011. [viitattu 13.3.2013]. Saatavissa: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/BNetzA/Sachgebiete/ Telekommunikation/Regulierung/Nummernverwaltung/TechnNummern/ITSI/ZuteilgsReglnITSI_TET-RAId4806pdf.pdf;jsessionid=3C3B296F574AEAAF47B30F49779D48C6?__blob=publicationFile

[32] Roelofsen, Gert: *Practical Security in TETRA*, In: IBC TETRA Conference. KPN Research, 2000. 14 s.

[33] Ruohonen, Mika. *Tietoturva*. 1 painos. Porvoo: Docendo Finland Oy. 2002. 428.s ISBN 951-846-163-5

[34] Singh, Simon. *Salakirjoituksen historia muinaisesta Egyptistä kvanttikryptografiaan*. Jyväskylä: Gummerrus kirjapaino Oy. 1999. 536 s. ISBN 951-31-1544-5

[35] Starr, Cheryl. *How to create a One Terafop Computer*.[viitattu 14.10.2012]. Saatavissa: http://www.ehow.com/how_6585908_create-one-teraflop-computer.html viitattu

[36] Suomisanakirja. *Iterointi.* [viitattu 14.10.2012] Saatavissa: www.suomisanakirja.fi/iterointi

[37] Valtiovarainministeriö. *Valtiohallinnon salauskäytännön tietoturvaohje*. 3/2008. Helsinki: Edita Prima Oy. 2008. 81 s. ISBN 978-951-804-806-3.

[38] Valtionvarainministeriö. *Valtionhallinnon tietoturvakäsitteistö.* Helsinki: Edita Prima Oy. 2003. 40 s. ISBN 951-804-404-8

[39] Valtionvarainministeriö. *Tunnistaminen julkishallinnon verkkopalveluissa.* Helsinki: Edita Prima Oy. 2006. 37 s. ISBN 951-804-669-7

[40] Vankka, Jouko. *Maavoimien taktisen verkon tekniikat ja standardit.* Viestikoulu. Helsinki: Edita Prima Oy. 2009. 383 s. ISBN 978-951-25-2025-1

[41] Vesanen, Ari. *Viranomasiverkoista*, [luentomateriaali]. Oulun yliopisto. 2003. [viitattu 9.9.2012]. Saatavissa: www.tol.oulu.fi/users/ari.vesanen/Langaton_TT/luennot/puhelin/Viranomaisverkot.html

[42] Viestintävirasto. *GSM-salausmenetelmä murrettu*. 2012 [viitattu 17.12.2012] Saatavissa: www.cert.fi/katsaukset/2012/tietoturvakatsaus_1-2012/gsm.html

[43] Viestintävirasto. *Tietoturvakatsaus 3/2011*. 2011 [viitattu 17.12.2012]. Saatavissa: www.cert.fi/katsaukset/2011/tietoturvakatsaus32011.html

LIITELUETTELO

LASKUT

1 Gigaflops = 10^9 Operaatiota sekunnissa

1 Teraflops = 10^{12} Operaatiota sekunnissa

1 Petaflops = 10^{15} Operaatiota sekunnissa

2^{64} operaatiota / (7,2 gigaflops) = ~2560000000 sekuntia = ~ 80 vuotta

2^{80} operaatiota / (7,2 gigaflops) = ~1,7 * 10^{14} sekuntia = ~ 50 000 000 vuotta

2^{64} operaatiota / (1 teraflops) = ~ 18500000 sekuntia = ~ 214 päivää

2^{80} operaatiota / (1 terafops) = ~sekuntia 1,21 * 10^{12} = ~ 38 000 vuotta

2^{64} operaatiota / (16 petaflops) = ~ 1152 sekuntia = ~ 20 minuuttia

2^{80} operaatiota / (16 petaflops) = ~ 75560000 sekuntia = ~ 2,4 vuotta

1,2 teraflopsia maksaa 279,10 € eli 1 teraflopsi maksaa noin 232,6 €. Lasketaan siis tarvittavien teraflopsien määrä ja kerrotaan se 232,6 €.